Formal Techniques and Tools
For Software Health Management

John Rushby (for N. Shankar)

Computer Science Laboratory

SRI International

Menlo Park CA USA

Introduction

- New project, just a few weeks old

- PI is Shankar, but he's at a conference in Korea
  - I'm a Co-Investigator,

- I was a member of the NRC Committee whose report "Sufficient Evidence" is cited in the NRA

- Report mentions Assurance/Dependability/Safety Cases

- I will talk about these tomorrow in IRAC track at 8am

- But, briefly. . .

Assurance Cases

- Intellectual basis for all assurance surely rests on

  ○ Claims or Goals, Evidence, Argument

- Standards-based assurance (e.g., DO-178B) specifies only
  the evidence to be produced

  ○ Claims and argument are largely implicit

- Assurance case: make all three items explicit

  ○ And also your confidence in each

Our Project, Generalities

- Health monitoring implies online checking

- We know how to do this (cf. Grigore Rosu)

- But what (source of) properties to monitor?

- Low Level SW requirements unlikely to be useful
  - DO-178B ensures these are implemented correctly

- Similarly with High Level SW requirements

- Most likely it's the requirements that are in error

- We need an independent source of properties to monitor

- Aha: the Assurance Case

Our Project, Particularities

- Derive monitors from formalized assurance cases

- Also monitor SW against its own history

    ○ Cf. anomaly detection

    ○ Identifies untested/novel scenarios

- Diagnosis: classical model-based

- Recovery/repair: first, use existing redundancy

    ○ Then, controller synthesis against the diagnostic model

- With explicit cognitive models of human operators

- Can do this because we have enormously powerful deductive systems

    ○ SMT solvers and their kin

- For more details, Google my paper "Runtime Certification"

Two Big Questions

- **Architectural** principles

- **Composability** (specifically, compositional certification)

- Profound insight (Tim Kelly):

  - The assurance case may not decompose along architectural lines

- **So what is an architecture**?

- A good one supports and enforces the assurance case

- Cf. **MILS approach to security**: next week at DASC

  - Explicitly compositional
  - Relates to IMA

Guarding the Guardians

- Fault tolerance is immensely hard

- Homespun solutions generally make things worse

- Our stuff will only kick in when existing fault tolerance and the certification process have failed

- So, we should have some humility

- Cf. AA 903 (1997): EFIS rebooted because roll rate was considered implausible
  - But pilots were attempting recovery from major upset
  - Loss of all instruments jeopardized this

- OTOH, A340 fuel emergency (2005), and 777 (2005) and A330 (2008) ADIRU incidents near Perth probably could have been mitigated by good SWHM

- Link to the assurance case seems the strongest guardian